OPSEC RISK ASSESSMENT

Operations Security (OPSEC)

OPSEC is the key to denial. It gives the commander the capability to identify those actions that can be observed by adversary intelligence systems. It can also provide an awareness of the potentially friendly indicators that adversary intelligence systems might obtain. The goal of OPSEC is to identify, select, and execute measures that eliminate, or reduce to an acceptable level, indications and other sources of information that may be exploited by an adversary. This documented method provides the framework for the systematic process necessary to identify, analyze, and protect information for essential secrecy. It uses a five-step process, which can be applied to any plan, operation, program, projects or activity. This process considers the changing nature of the threat and friendly vulnerabilities throughout the operations and if initiated can provide adequate protection toward the overall mission effectiveness.

OPSEC Observations

Identify each OPSEC vulnerability to the organization. The "Analysis of Vulnerabilities" is an examination of an operation to determine the information and sources of information available to adversaries. Critical information may be derived by adversaries from various sources if the sources are not controlled. An OPSEC vulnerability exists when these three conditions are met:

- An adversary has the capability to collect the indicator.
- The adversary has the time to collect, report, analyze and make a decision.
- The adversary can react or take an action that will be harmful to Organization.

Program: This category is defined as all vulnerabilities encompassed by failure to develop an OPSEC program that identifies organization critical information and provides for adequate safeguards against unintentional release of that information; identify adversary capabilities and implementing protective measures. Planning guidance is an essential element of an OPSEC Program. There is no set format for an OPSEC Plan. However, at a minimum it must address the following:

- Requirements for essential secrecy about friendly intentions and military capabilities
- Tasks to staff and subordinate commands to plan and implement OPSEC measures
- OPSEC estimate comprising identified or assumed adversary knowledge, EEFI, and evaluation of OPSEC effectiveness
- OPSEC threat consisting of detectable activities and the adversary's capability to obtain information
- OPSEC measures to implement

The OPSEC Officer is responsible for directing and implementing the OPSEC program. The OPSEC Officer should be:

- appointed on orders,
- a member of the unit's operations staff
- the rank of CPT or above, CW2 or above, SFC or above, GS-9 or above, and
- trained in the use of OPSEC analytic techniques to identify vulnerabilities and to select appropriate OPSEC measures.

OPSEC Program	Critical	High	Medium	Low
OPSEC Plan				
OPSEC Officer				

Unit Training and Awareness: OPSEC training programs should ensure that all personnel are aware of adversary intelligence threats and understand the OPSEC process. The individual vulnerabilities that result from not establishing a training and awareness program that disseminates the units' Essential Elements of Friendly Information (EEFI) to the lowest level and identifies the adversary capabilities are assessed below.

Unit Awareness	Critical	High	Medium	Low
Training and Awareness				

Information Identification: The documented method of implementing protective measures to protect the units' critical information.

Information Identification	Critical	High	Medium	Low
Development of EEFI				
Identify Adversary and Collection Capability				
Identify Indicators, Vulnerabilities and Protective Measures				
Implementing OPSEC Measures				
Synchronize OPSEC with other IO Elements				

OPSEC Risk Analysis

Risk analysis revealed that action control OPSEC measures should be implemented to mitigate the risk associated with most Organization vulnerabilities.

The most probable vulnerabilities fall in the areas of:

MATRIX OF OPSEC VULNERABILITIES

Vulnerabilities	THREATS						
	FIS	Terrorist	Criminals	Protesters	Subversives	Hackers	Individuals
Email	X	X	X	X	X	X	X
Telephone/cell phones	X	X	X			X	X
Web-sites	X	X	X	X	X	X	X
Lack of OPSEC training		X		X		X	X
Trash	X	X	X	X	X	X	X

The figure below provides a tool which may be used to document the threat levels relative to Organization's assets and related undesirable events and their impacts. The threat levels identified on the chart are based on MDCI threat to Organization, dated 5 September 2003.

Critical Asset	Undesirable Event/Impact	Threat/ Adversary	Overall Risk
OPSEC Program	▪ Lack of OPSEC Program ⇨ Critical information vulnerable	ALL THREATS	
	▪ Lack of OPSEC Leadership ⇨ Capability disclosures	FIS-HUMINT	
	▪ Poor OPSEC practices ⇨ OPSEC violations not noticed or reported	Insiders OSINT Criminal	
	▪ Lack of OPSEC training ⇨ Unauthorized release/Disclosure of capabilities	Insiders Subversives	
	▪ Lack of OPSEC awareness ⇨ Loss of critical information	Terrorist	
	▪ EEFI not developed ⇨ Critical information not protected	OSINT	
	▪ Threat/Adversary not Determined ⇨ Exploitation by all adversaries	FIS-HUMINT FIS-SIGINT	
	▪ OPSEC Indicators and Vulnerabilities not Identified ⇨ Observation of operations by all adversaries	FIS-HUMINT/ SIGINT Terrorist	
	▪ Stand-off technical attack ⇨ Compromise of critical information	Hackers FIS-SIGINT	
	▪ Poor OPSEC ⇨ Loss or compromise of critical information	FIS Insiders OSINT	

OPSEC measures are chosen by the commander and incorporated into ongoing or planned activities. Effective OPSEC requires disseminating OPSEC guidance to every soldier. Good OPSEC involves telling soldiers why OPSEC measures are important and what they are designed to accomplish. All personnel must understand the cost of failing to maintain effective OPSEC. Understanding why they are doing something and what their actions are supposed to accomplish motivates soldiers to execute tasks more effectively. Active and deliberate actions by soldiers are crucial to successful OPSEC.

The following **Action Control** OPSEC measures are identified for each Organization OPSEC vulnerability as indicated. OPSEC measures should be monitored to ensure that a measure to protect a specific piece of critical information does not unwittingly provide information to an adversary.

Undesirable Event	**Existing Risk Level**	**Related Vulnerabilities**	**OPSEC Measure Options**	**Reduced Risk Level**
Lack of OPSEC Program		Critical information vulnerable	Develop OPSEC Plan	
Lack of OPSEC Leadership		Disclosure of capabilities Poor OPSEC	Appoint OPSEC officer	
Poor OPSEC practices		OPSEC violations not noticed or reported	Command emphasis	
Lack of OPSEC training		Unauthorized release/Disclosure of capabilities	Conduct initial and annual training	
Lack of OPSEC awareness		Lost of critical information	Conduct initial and annual training	
EEFI not developed		Critical information not protected	Develop EEFI down to Battalion level	
Threat/Adversary not Determined		Exploitation by all adversaries	Coordinate with G-2 to identify adversaries and their collection capabilities	
OPSEC Indicators and Vulnerabilities not Identified		Observation of operations by all adversaries	Identify all detectable indicators and apply OPSEC measures	
Stand-off technical attack		Compromise of critical information	Better password controls	
Poor OPSEC		Loss or compromise of critical information	OPSEC awareness training